Sur le nombre de points rationnels des varietes abeliennes et des Jacobiennes sur les corps finis

Yves Aubry, Safia Haloui, Gilles Lachaud

Sur le nombre de points rationnels des variétés abéliennes et des Jacobiennes sur les corps finis

Yves Aubry [a,b], Safia Haloui [a,c], Gilles Lachaud [a]

[a] *Institut de Mathématiques de Luminy, Aix-Marseille Université-CNRS, France*
[b] *Institut de Mathématiques de Toulon, Université du Sud Toulon-Var, France*
[c] *Department of Mathematics, Technical University of Denmark, Lyngby, Denmark*

Reçu le ** août 2012 ; accepté après révision le ***

Présenté par Jean-Pierre Serre

Résumé

Nous établissons de nouvelles bornes inférieures et supérieures sur le nombre de points rationnels des variétés abéliennes et des Jacobiennes sur un corps fini. Nous déterminons de plus les nombres maximum et minimum de points rationnels des surfaces Jacobiennes. *Pour citer cet article : Y. Aubry, S.Haloui, G. Lachaud, C. R. Acad. Sci. Paris, Ser. I xxx (2012).*

Abstract

On the number of points on abelian and Jacobian varieties over finite fields. *To cite this article: Y. Aubry, S.Haloui, G. Lachaud, C. R. Acad. Sci. Paris, Ser. I xxx (2012).*

1. Variétés abéliennes

Soit A une variété abélienne de dimension g définie sur le corps fini $\mathbb{F}_q$ de caractéristique p, avec $q = p^n$. Le *polynôme de Weil* $f_A(t)$ de A est le polynôme caractéristique de son endomorphisme de Frobenius F_A. On note $\omega_1, \ldots, \omega_g, \overline{\omega}_1, \ldots, \overline{\omega}_g$ les racines complexes de $f_A(t)$ et $|\omega_i| = q^{1/2}$. Pour $1 \leq i \leq g$, on pose $x_i = -(\omega_i + \overline{\omega}_i)$, et on dit que A est de *type* $[x_1, \ldots, x_g]$. Le type de A dépend uniquement de sa classe d'isogénie. On note $\tau = \tau(A) = -\sum_{i=1}^{g}(\omega_i + \overline{\omega}_i) = \sum_{i=1}^{g} x_i$ l'opposé de la trace de F_A et on dit que A est de *trace* $-\tau$. Le nombre de points rationnels de A sur $\mathbb{F}_q$ est donné par

Email addresses: yves.aubry@univ-tln.fr (Yves Aubry), s.haloui@mat.dtu.dk (Safia Haloui), lachaud@univ-amu.fr (Gilles Lachaud).

$$|A(\mathbb{F}_q)| = f_A(1) = \prod_{i=1}^{g}(q+1+x_i). \tag{1}$$

Puisque $|x_i| \leq 2q^{1/2}$, on déduit de (1) les bornes classiques :

$$(q+1-2q^{1/2})^g \leq |A(\mathbb{F}_q)| \leq (q+1+2q^{1/2})^g.$$

Ces bornes peuvent être améliorées :

Théorème 1.1 *Soit A une variété abélienne définie sur $\mathbb{F}_q$ de dimension g, et posons $m = [2\sqrt{q}]$. Alors*

$$(q+1-m)^g \leq |A(\mathbb{F}_q)| \leq (q+1+m)^g$$

avec égalité à droite (resp. à gauche) si et seulement si A est de type $[m,\ldots,m]$ (resp. $[-m,\ldots,-m]$).

On peut être plus précis en introduisant la trace :

Théorème 1.2 *Soit A une variété abélienne définie sur $\mathbb{F}_q$ de dimension g et de trace $-\tau$. Alors*

$$|A(\mathbb{F}_q)| \leq \Big(q+1+\frac{\tau}{g}\Big)^g,$$

avec égalité si et seulement si A est de type $[\tau/g,\ldots,\tau/g]$.

Ce résultat a été démontré par H.G. Quebbemann [5] pour les Jacobiennes et par M. Perret [4] pour les variétés de Prym. On dit que A (ou τ) est de *défaut* d si $\tau = gm - d$. On a :

Proposition 1.3 *Si A est de défaut d, avec $d = 1$ ou $d = 2$, alors*

$$|A(\mathbb{F}_q)| \leq (q+m)^d(q+1+m)^{g-d}.$$

On s'attache maintenant à déterminer une borne inférieure pour $|A(\mathbb{F}_q)|$ symétrique de la borne supérieure du Théorème 1.2, et qui dépend du *quotient de Specht* défini pour $h \geq 1$ par

$$S(h) = \frac{h^{1/(h-1)}}{e\log h^{1/(h-1)}}, \quad S(1) = 1.$$

Théorème 1.4 *Si $q \geq 2$, posons $M(q) = 1/S(h(q))$ et $h(q) = \big((q^{1/2}+1)/(q^{1/2}-1)\big)^2$. Soit A une variété abélienne définie sur $\mathbb{F}_q$ de dimension g et de trace $-\tau$. Alors*

$$|A(\mathbb{F}_q)| \geq M(q)^g\Big(q+1+\frac{\tau}{g}\Big)^g.$$

De plus $M(2) \geq 0.261$ et $M(q) \geq 1-(2/q)$.

Théorème 1.5 *Soit A une variété abélienne définie sur $\mathbb{F}_q$ de dimension g et de trace $-\tau$. Alors*

$$|A(\mathbb{F}_q)| \geq (q+1-m)^g + (q-m)^{g-1}(gm+\tau).$$

Une autre façon d'obtenir des bornes inférieures pour $|A(\mathbb{F}_q)|$ est d'utiliser des méthodes de convexité comme M. Perret dans [4]. On obtient :

Proposition 1.6 *Posons $r = [(g+[\omega])/2]$ et $s = [(g-1-[\omega]/2]$, où $\omega = \tau/(2q^{1/2})$. Alors*

$$|A(\mathbb{F}_q)| \geq (q+1+\tau-2(r-s)q^{1/2})(q+1+2q^{1/2})^r(q+1-2q^{1/2})^s.$$

On démontre également de nouvelles minorations de $|A(\mathbb{F}_q)|$ en fonction de la *moyenne harmonique* $\eta = \eta(A)$ des nombres $q+1+x_i$, qui est définie par :

$$\frac{1}{\eta} = \frac{1}{g}\sum_{i=1}^{g}\frac{1}{q+1+x_i} = \frac{1}{g}\sum_{i=1}^{g}\frac{1}{|1-\omega_i|^2}\,.$$

Théorème 1.7 *Soit A une variété abélienne définie sur $\mathbb{F}_q$ de dimension g. Alors $|A(\mathbb{F}_q)| \geq \eta(A)^g$.*

On démontre que si $q \geq 8$, alors $\eta(A) \geq q+1-m$. Le Théorème 1.7 est donc plus précis que le Théorème 1.1 si $q \geq 8$. Notons que si $q \leq 7$, on peut avoir $\eta(A) < q+1-m$.

2. Jacobiennes

On considère une courbe algébrique C, projective, non singulière, définie sur $\mathbb{F}_q$ et absolument irréductible. On note J_C sa Jacobienne et $N = |C(\mathbb{F}_q)|$ son nombre de points rationnels sur $\mathbb{F}_q$. Les résultats de la section 1 s'appliquent évidemment aux Jacobiennes ; en particulier, le Théorème 1.4 implique :

Proposition 2.1 *Si C est une courbe comme ci-dessus de genre g, alors :*

$$|J_C(\mathbb{F}_q)| \geq M(q)^g \Big(q + 1 + \frac{N - (q+1)}{g}\Big)^g.$$

Les Propositions 1.5 et 1.6 fournissent des bornes sur les Jacobiennes de la même manière.

On s'intéresse à présent aux variétés abéliennes possédant certaines propriétés, les Jacobiennes en étant des exemples particuliers. Si A est une variété abélienne définie sur $\mathbb{F}_q$ de dimension g, on note $P(t) = P_A(t)$ le polynôme réciproque de son polynôme caractéristique $f_A(t)$. On définit la *fonction zêta virtuelle* de numérateur $P(t)$ comme la série formelle :

$$Z(t) = \frac{P(t)}{(1-t)(1-qt)} \in \mathbb{Z}[[t]]\,.$$

On définit trois suites (A_n), (B_n), (N_n) par les identitées suivantes :

$$Z(t) = \sum_{n=0}^{\infty} A_n t^n = \exp \sum_{n=1}^{\infty} N_n \frac{t^n}{n} = \prod_{n=1}^{\infty} (1-t^n)^{-B_n}. \tag{2}$$

Comme on l'a démontré dans [3] avec la fonction zêta d'une courbe, on a

Théorème 2.2 *Supposons $g \geq 2$. Avec les notations précédentes,*

$$\frac{g}{\eta(A)}\,|A(\mathbb{F}_q)| = \sum_{n=0}^{g-1} A_n + \sum_{n=0}^{g-2} q^{g-1-n} A_n. \quad \square$$

Si $A = J_C$ est la Jacobienne d'une courbe C sur $\mathbb{F}_q$, alors A_n et B_n représentent respectivement les nombres de diviseurs rationnels effectifs et premiers de degré n de C, et $N_n = |C(\mathbb{F}_{q^n})|$. Dans ce cas, les deux conditions suivantes sont vérifiées :

$$B_n \geq 0 \qquad \text{si} \quad 1 \leq n \leq 2g, \tag{\textbf{B}}$$

$$N_n \geq N_1 \geq 0 \quad \text{si} \quad 1 \leq n \leq 2g. \tag{\textbf{N}}$$

En fait, ces conditions sont vérifiées pour tout $n \geq 1$. La proposition suivante, qui améliore certains résultats de N. Elkies & al. [1], montre que les conditions (**B**) et *a fortiori* (**N**) sont propres aux Jacobiennes seulement si g est grand devant q.

Proposition 2.3 *Soit A une variété abélienne définie sur $\mathbb{F}_q$ de dimension $g \geq 1$. Si $n \geq 2$, alors*

$$nB_n \geq (q^{n/4}+1)^2((q^{n/4}-1)^2 - 2g).$$

Le théorème suivant s'applique évidemment aux Jacobiennes.

Théorème 2.4 *Soit A une variété abélienne définie sur $\mathbb{F}_q$ de dimension $g \geq 2$. Si la condition* (**B**) *est vérifiée, alors*

$$|A(\mathbb{F}_q)| \geq \frac{q-1}{q^g - 1}\left[\binom{N+2g-2}{2g-1} + \sum_{n=0}^{2g-3} B_{2g-1-n}\binom{N+n-1}{n}\right].$$

Si la condition (**N**) *est vérifiée, alors*

$$|A(\mathbb{F}_q)| \geq \frac{\eta(A)}{g}\left[\binom{N+g-2}{g-2} + \sum_{n=0}^{g-1} q^{g-1-n}\binom{N+n-1}{n}\right].$$

Si la condition (**N**) *est vérifiée, et si* $N \geq g(q^{1/2}-1)+1$, *alors*

$$|A(\mathbb{F}_q)| \geq \binom{N+g-1}{g} - q\binom{N+g-3}{g-2}.$$

3. Surfaces Jacobiennes

On s'intéresse au nombre maximum et minimum de points rationnels de la Jacobienne d'une courbe de genre 2. On définit pour cela les quantités $J_q(2) = \max_C |J_C(\mathbb{F}_q)|$ et $j_q(2) = \min_C |J_C(\mathbb{F}_q)|$, où C décrit l'ensemble des courbes lisses sur $\mathbb{F}_q$ de genre 2.

La détermination de ces quantités implique une connaissance précise des classes d'isogénies des surfaces abéliennes qui contiennent une Jacobienne, ce qui a été fait par E. Howe, E. Nart, and C. Ritzenthaler dans [2].

Rappelons qu'un nombre qui est une puissance impaire q d'un premier p est *spécial* si $p|m$ ou s'il existe une solution entière à l'une des équations $q = x^2+1$, $q = x^2+x+1$, $q = x^2+x+2$.

Théorème 3.1 *On a*

$$j_q(2) = (q+1-m)^2, \quad J_q(2) = (q+1+m)^2,$$

sauf dans les cas particuliers suivants :

$j_q(2)$	q *carré*	$q=4$	5
		$q=9$	25
	q *spécial*	$\{2q^{1/2}\} \geq \varphi_1$	$(q+1-m-\varphi_1)(q+1-m-\varphi_2)$
		$\sqrt{2}-1 \leq \{2q^{1/2}\} < \varphi_1$	$(q+2-m+\sqrt{2})(q+2-m-\sqrt{2})$
		$\{2q^{1/2}\} < \sqrt{2}-1$, $p \not| m$, $q \neq 7^3$	$(q+1-m)(q+3-m)$
		sinon	$(q+2-m)^2$
$J_q(2)$	q *carré*	$q=4$	55
		$q=9$	225
	q *spécial*	$\{2q^{1/2}\} \geq \varphi_1$	$(q+1+m+\varphi_1)(q+1+m+\varphi_2)$
		$\{2q^{1/2}\} < \varphi_1$, $p \neq 2$ *ou* $p|m$	$(q+m)^2$
		sinon	$(q+1+m)(q-1+m)$

Ici $\varphi_1 = (-1+\sqrt{5})/2$, $\varphi_2 = (-1-\sqrt{5})/2$ *et* $\{a\}$ *est la partie fractionnaire du nombre* a.

Références

[1] Elkies, Noam D. ; Howe, Everett W. ; Kresch, Andrew ; Poonen, Bjorn ; Wetherell, Joseph L. ; Zieve, Michael E. Curves of every genus with many points. II. Asymptotically good families. *Duke Math. J.* **122** (2004), no. 2, 399–422.

[2] Howe, Everett ; Nart, Enric ; Ritzenthaler, Christophe. Jacobians in isogeny classes of abelian surfaces over finite fields. *Ann. Inst. Fourier* **59** (2009), 239–289.

[3] Lachaud, Gilles ; Martin-Deschamps, Mireille. Nombre de points des jacobiennes sur un corps fini. *Acta Arithmetica* **16** (1990), 329–340.

[4] Perret, Marc. Number of points of Prym varieties over finite fields. *Glasgow Math. J.* **48** (2006), 275–280.

[5] Quebbemann, Heinz-Georg. *Lattices from curves over finite fields.* Preprint (April 1989).